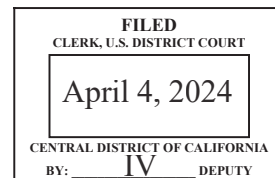




UNITED STATES DISTRICT COURT

for the

Central District of California



United States of America,

v.

CHRISTIAN ROBERTO FLORES,

Defendant

Case No. 2:24-mj-01997

**CRIMINAL COMPLAINT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 3, 2024 in the county of Los Angeles in the Central District of California,
the defendant(s) violated:

Code Section

18 U.S.C. § 922(g)(1)

Offense Description

Felon in Possession of a Firearm

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ James Bewley

Complainant's signature

James Bewley, HSI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: April 4, 2024

Patricia Donahue

Judge's signature

City and state: Los Angeles, California

Hon. Patricia Donahue, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, James Bewley, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against CHRISTIAN ROBERTO FLORES ("FLORES") for a violation of Title 18 U.S.C. § 922(g)(1): Felon in Possession of a Firearm.

2. This affidavit is also made in support of an application for a warrant to search the following digital devices in the custody of Homeland Security Investigations ("HSI") in El Segundo, California, (collectively, the "SUBJECT DEVICES"), all seized on April 3, 2024, from 24615 Eshelman Avenue, Lomita, California, (the "Subject Premises" or the "FLORES residence") as described more fully in Attachment A:

a. A Black Apple iPhone, seized from FLORES's person ("SUBJECT DEVICE 1");

b. a thumb drive, seized from the detached shed on the Subject Premises ("SUBJECT DEVICE 2");

c. a thumb drive that looked like a key, seized from the detached shed on the Subject Premises ("SUBJECT DEVICE 3");
and

d. a storage device, seized from the detached shed on the Subject Premises ("SUBJECT DEVICE 4").

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 922(g)(1) (Felon in Possession of a Firearm and Ammunition) and 26 U.S.C. § 5861 (Unlawful Manufacture, Transfer

or Possession of an Unregistered Firearm) (the "Subject Offenses"), as described more fully in Attachment B.

4. Attachments A and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

6. I am a HSI Special Agent and have been so employed since September 2020. I am currently assigned to the HSI Los Angeles International Airport Regional Illegal Firearms Trafficking Team ("RIFTT") where I investigate violations of immigration and customs laws, including the illegal manufacture, importation, exportation, and trafficking of firearms and silencers into the United States in violation of the National Firearms Act.

7. I am a graduate of the Federal Law Enforcement Training Center in Glynco, Georgia. While there, I completed courses that cover criminal investigative functions, criminal law, immigration law, and customs law, as well as additional

training specifically related to the investigation into firearms and related offenses.

8. From working with the RIFTT, I have gathered experience and knowledge in the identification, nomenclature and functionality of firearms, firearms silencers, short-barreled firearms, and add-on firearm components. I have also participated in multiple federal and state search warrants related to silencers and other firearms-related violations.

9. I also currently serve as a reservist in the United States Marine Corps, where I serve as an Artillery Officer. During my service, I was trained and familiarized myself with various firearms and weapon systems. Those weapons and firearms systems include pistols, rifles, machineguns, grenade launchers, and crew served weapons. I was also trained in the employment of these firearms and weapon systems.

III. SUMMARY OF PROBABLE CAUSE

10. On April 3, 2024, law enforcement executed a search warrant at the Subject Premises where they found multiple firearms, suspected silencers, ammunition, and suspected explosive devices inside of FLORES's bedroom. Agents also found indicia of firearms manufacturing inside of a shed, including three pistol lower receivers, a 3D resin printer, and a 3D-printer. At the time, FLORES was prohibited from possessing firearms and ammunition because he had been convicted of several felony offenses, including drug and gun crimes.

IV. STATEMENT OF PROBABLE CAUSE

11. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Background of the Investigation

12. On August 3, 2023, CBP seized a shipment of undeclared firearm-related items. They seized 572 Glock switches,¹ 180 suspected silencers, and 76 silencer parts and accessories, bound for the 4PX Warehouse in Commerce, California.

13. On August 30, 2023, HSI searched the 4PX Warehouse pursuant to federal search warrant 2:23-MJ-04419 and seized firearm-related items such as 17 suspected Glock switches, 108 suspected auto sears, 256 suspected firearm silencers, among other things.

14. On August 23, 2023, I served a customs summons at the 4PX Warehouse in Commerce, California requiring 4PX Express to produce their shipment records. In response, 4PX provided a report detailing recent shipments from the 4PX Warehouse to various locations in the United States. This report detailed the items 4PX shipped, where and when 4PX had shipped the items, and who 4PX was shipping the items to.

¹ A Glock switch is a device that can be installed into a semi-automatic firearm that makes the weapon function as a machinegun. The Glock switch itself is considered a machinegun under relevant federal law.

15. From my review of that report, I am aware that on May 13, 2023, 4PX shipped a Nielsen Device² to FLORES at 24615 Eshelman Avenue, Lomita, California. The report also listed FLORES's phone number ending in -9736.

16. On January 22, 2024, using law enforcement databases, law enforcement learned that FLORES was listed as living at the FLORES residence, and that the phone number ending in -9736 was associated with FLORES.

17. Based on a review of law enforcement databases, law enforcement learned that FLORES had felony convictions, including for illegally possessing firearms. In 2013, FLORES was convicted of being in possession of a short-barreled rifle in violation of California Penal Code section 33215, and in 2020 he was convicted of being a felon in possession of a firearm, in violation of California Penal Code section 29800(a)(1).

18. Law enforcement queried FLORES in the Automated Firearms System and learned that FLORES did not have a firearm registered to him.

B. Law Enforcement Searched the FLORES Residence and Found Firearms, Ammunition, and Suspected Silencers

19. From my review of reports, discussions with other law enforcement personnel, and my own knowledge of the investigation, I am aware of the following:

² Based on my training and experience, I am aware that a Nielsen Device is a firearm add-on part that helps semi-automatic pistols cycle when a suppressor is attached. The Nielsen Device's sole purpose is to be fitted into a handgun and used in conjunction with a silencer.

a. On March 29, 2024, law enforcement obtained a California state search warrant signed by Superior Court Judge PJ Mirich authorizing the search of FLORES's residence and person. On April 3, 2024, at 4:00 a.m., HSI and LAPD executed the search warrant on the FLORES Residence.

b. Law enforcement personnel loudly announced their police presence and their intent to serve a search warrant. FLORES's mother, D.C., opened the door. FLORES's daughter, brother, and grandmother were also at the Subject Premises.

c. The Subject Premises consisted of the main house, which was closest to the street, a detached shed, and detached living quarters behind the shed.



d. Law enforcement searched the detached living quarters and found firearms and firearm-related contraband. Specifically, law enforcement found:

i. A Nielson Device, which was identical to the one the 4PX Warehouse had shipped to FLORES;

ii. A short-barrel rifle³ without a serial number;

iii. A Winchester Model 1400 12-gauge short-barreled shotgun, serial number N453946, engraved with language stating that it was "made in New Haven, Conn.";

iv. A pistol with a threaded barrel without a serial number inside a Glock pistol box on the ground in plain view;

v. Three suspected silencers;

vi. A homemade suspected silencer on the bed in plain view;

vii. Four homemade pyrotechnic devices, two of which were found in the top drawer of the dresser;

viii. Approximately 420 rounds of ammunition;

ix. Three 30-round high-capacity magazines;

x. Two rifle magazines;

xi. Four 10-round 9mm pistol magazines;

xii. A 15-round high-capacity 9mm magazine; and

xiii. One firearm magazine.

20. Law enforcement also found indicia that FLORES lived in the detached living room quarters, specifically a document in FLORES's name and a California ID in his name.

³ As discussed further in Section IV.E., on April 3, 2024, an ATF firearms expert informed me that the rifle was a short-barrel rifle, the shotgun was a short-barrel shotgun, and that the three suspected silencers were indeed silencers.

21. While LAPD was searching the detached living quarters, law enforcement interviewed FLORES' mother. She stated that FLORES did not live at the residence but that he would come over after his work shift, go into the detached living quarters, and stay there until he would leave later at night. She stated that she does not go into FLORES's room because he does not allow her in there and keeps it locked.

22. Law enforcement also searched the detached shed and found the following items:

- a. Three pistol lower receivers, at least two of which were printed;
- b. A 3D printer;
- c. A 3D resin printer;
- d. SUBJECT DEVICE 2, which was plugged into the 3D resin printer;
- e. SUBJECT DEVICE 3, which was next to the 3D resin printer; and
- f. SUBJECT DEVICE 4, which was on the 3D resin printer.

23. Based on my training and experience, I believe that the resin 3D printer created at least two of the pistol lowers because a resin 3D printer produces finer detail in the items it prints, which matched the level of detail found in the pistol lowers.

C. Officers Arrest FLORES

24. At approximately 10:00 a.m., law enforcement saw FLORES on the street near the FLORES Residence. At the time of FLORES's arrest, he possessed SUBJECT DEVICE 1 on his person.

25. Law enforcement attempted to interview FLORES on scene and he invoked his right to counsel.

D. FLORES is a Convicted Felon

26. Based on my review of FLOWERS's criminal history records, I know that he has previously been convicted of the following felony crimes punishable by a term of imprisonment exceeding one year:

a. On or about May 28, 2013, Possession of a Short-Barreled Rifle, in violation of California Penal Code section 33215 and Domestic Violence, in violation of California Penal Code section 273.5(A), in Case Number YA087381 in the Superior Court for the State of California;

b. On or about January 26, 2016, Possession of Narcotics for Sale, a violation of California Health and Safety Code section 11351; Possession of Methamphetamine with Intent to Sell, a violation of California Health and Safety Code section 11378; and Possession of Illegal Explosives, in violation of California Health and Safety section 12305, in Case Number LB1140101 in the Superior Court for the State of California;

c. On or about October 28, 2020, Felon in Possession of a Firearm, in violation of California Penal Code section 29800(A)(1) PC, Case Number XSWYA10098201 in the Superior Court for the State of California; and

d. On or about October 28, 2020, Possession of Methamphetamine with Intent to Sell, a violation of California Penal Code section 11378, in Case Number SBAYAYA10232301 in the Superior Court for the State of California.

E. Interstate Nexus and Analysis of Seized Items

27. Based on my conversation with an ATF Interstate Nexus Expert, I am aware that on April 3, 2024, he examined the short-barreled shotgun bearing serial number N453946 and the short-barreled rifle via photographs and determined the following:

a. The Winchester Model 1400 12-gauge short-barreled shotgun, serial number N453946, was manufactured outside of the state of California and therefore traveled in interstate commerce, as it was recovered in California.

b. The short-barreled rifle and the short-barreled shotgun qualify as short-barreled firearms under the National Firearms Registry because the rifle had a barrel under 16 inches and the shotgun had a barrel under 18 inches.

28. From my conversation with an ATF Firearms Enforcement Officer, I am aware that on April 3, 2024, he examined photographs of three of the suspected silencers and determined that they are silencers.

V. TRAINING AND EXPERIENCE ON FIREARMS OFFENSES

29. From my training, personal experience, and the collective experiences related to me by other law enforcement officers who conduct who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that the sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they

or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

30. As used herein, the term "digital device" includes the SUBJECT DEVICES.

31. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

32. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

33. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

//

//

VII. CONCLUSION

34. For all of the reasons described above, there is probable cause to believe that CHRISTIAN ROBERTO FLORES has committed a violation of 18 U.S.C. § 922(g)(1): Felon in Possession of a Firearm. There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES described in Attachment A.

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 4th day of April
2024.



THE HONORABLE PATRICIA DONAHUE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital devices (the "SUBJECT DEVICES"), seized on April 3, 2024, all seized on April 3, 2024, and currently maintained in the custody of Homeland Security Investigations in El Segundo, California:

a. Black Apple iPhone, seized from FLORES's person ("SUBJECT DEVICE 1");

b. A thumb drive, seized from the detached shed on the Subject Premises ("SUBJECT DEVICE 2");

c. A thumb drive that looked like a key, seized from the detached shed on the Subject Premises ("SUBJECT DEVICE 3"); and

d. A storage device, seized from the detached shed on the Subject Premises ("SUBJECT DEVICE 4").

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code Section 922(g) (Felon in Possession of a Firearm) and Title 26, United States Code 5861 (Unlawful Manufacture, Transfer or Possession of an Unregistered Firearm) (the "Subject Offenses") namely:

a. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violation;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

d. Records, documents, programs, applications, materials, or conversations relating to the sale or purchase of guns or ammunition, including correspondence, receipts, records, and documents noting prices or times when guns or ammunition were bought, sold, or otherwise distributed;

e. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of guns or ammunition;

f. Contents of any calendar or date book;

g. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

h. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

i. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

3. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICES as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital devices beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or

encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies

of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICES, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not

apply to any search of digital devices pursuant to any other court order.